Desarrollo Seguro

Lección 3: Controles Pro-activos

eip ESCUELA INTERNACIONAL POSGRADOS

Indice

Introducción

En la presente lección se han trato los controles de seguridad pro-activos, aquellos que se aplican de manera activa para evitar ataques o poner todos los impedimentos posibles para que estos sean realizados de forma exitosa por lo tanto en la actividad que refiere a esta lección se pide analizar un pequeño programa y justificar los controles pro-activos aplicables así como las recomendaciones de la guía de seguridad de las TIC CCN-STIC 857.

Controles Pro-activos

OWASP TOP 10

C6: Identidad Digital

Al leer la practica se establece que el acceso al formulario se realiza mediante autenticación multifactor, es decir, se emplea una contraseña y el móvil al que se envía una clave mediante una aplicación. En las aplicaciones de nivel dos también es recomendado emplear una huella biométrica para el inicio de sesión sin embargo, podemos asumir que el acceso al móvil en cual se mostrará la clave de acceso se realiza mediante una huella dactilar o reconocimiento facial lo cual establece el tercer punto de acceso para aplicaciones de seguridad de nivel dos.

C2: Aprovechar frameworks y bibliotecas de seguridad

Al crear la aplicación se empleará dash como framework principal ya que es un framework que actualmente continua recibiendo actualizaciones y proviene de una fuente conocida como es la librería pip de python además, se realizarán revisiones periódicas del código a fin de mantenerlo actualizado.

C3: Acceso seguro a la base de datos

Ya que hay que acceder a una base de datos se ha de asegurar que este acceso sea completamente seguro para ello aseguraremos que toda consulta que se realice sea mediante un usuario autenticado.

C5: Validar todas la entradas

Como se ha comentado anteriormente, hay que realizar una consulta a una base de datos y tras esto se modificarán o añadirán datos a la misma de forma que para reforzar el punto anterior, C3, se realizará una verificación de todas la entradas, de forma que todos los datos enviados a la base de datos sean del tipo correcto y no contengan caracteres no deseados o no permitidos que puedan ser fuente de un ataque del tipo inyección de SQL.

C7: Aplicar controles de acceso

Además del control de autenticación, se verificará que el usuario que ha solicitado la consulta a la base de datos tenga permiso para realizarla. Esto reducirá la cantidad de usuarios con acceso a la base de datos reduciendo el área de ataque.

TIC CCN-STIC 857

Con los controles pro-activos de la lista OWASP TOP 10 la mayor parte de las Amenazas[T] consideradas en la guía TIC CCN-STIC 857 quedan cubiertas. Otras como puede ser T.Interceptación podrían generar algún tipo de problema si la red de comunicaciones flaquea y permite ataques del tipo “Man in the Middle” con lo que podría quedar alguna clave al descubierto sin embargo, dado que se ha restringido el acceso al formulario a unos pocos usuarios, y los que tienen acceso han de autenticarse dos veces, el éxito de un ataque de este estilo se reduce drásticamente. Sin embargo, podría reducirse aun mas el riesgo implementando cambios de contraseña periódicos.

Por otra parte, las políticas de seguridad tratan temas que ya se han tenido en cuenta en el apartado anterior a excepción de P.BackendLog que seria necesario implementarlo ya que la información de ataques pasados es muy útil a la hora de corregir agujeros que no se hayan tenido en cuenta en análisis anteriores.